On the Secrecy Capacity of the Z-Interference Channel

Ronit Bustin
Dept. of Electrical Engineering
Tel Aviv University
Email: ronitbustin@post.tau.ac.il

Mojtaba Vaezi
Dept. of Electrical Engineering
Princeton University
Email: mvaezi@princeton.edu

Rafael F. Schaefer
Information Theory and Applications Group
Technische Universität Berlin
Email: rafael.schaefer@tu-berlin.de

H. Vincent Poor
Dept. of Electrical Engineering
Princeton University
Email: poor@princeton.edu

***Abstract*—The two-user Z-interference channel with an additional secrecy constraint is considered. The two transmitter-receiver pairs wish to reliably transmit their messages; however the transmission of the first pair both interferes with the transmission of the second pair and is also required to be completely secure from the second receiver. The focus here is on the capacity region of the above Z-interference channel in the Gaussian case under the standard power constraints. The maximum rates of the two users in this setting are described, and although the maximum rate of the transmission of the first pair has a single-letter expression, due to Wyner's secrecy capacity expression, its maximization is non-trivial. The significance of a stochastic encoder for the second transmitter, encoding a message which is not required to comply with any secrecy constraints, is noted. It is shown explicitly that constraining this encoder to be deterministic reduces the capacity region. Finally, a Sato-type outer bound on the capacity region is obtained under this additional deterministic encoder constraint.**

I. Introduction

The interference channel is a central open problem in multi-user information theory. Understanding the effect of interference is critical to the understanding of the limitations of communication and essentially the interactions in any network. The basic aspects of interference appear already in the simplest setting - the two-user Z-interference channel. This channel comprises two independent inputs $(\boldsymbol{X}_1, \boldsymbol{X}_2)$ and two outputs $(\boldsymbol{Y}_1, \boldsymbol{Y}_2)$ (throughout the paper bold letters denote length n random vectors) with a channel conditional distribution of the following form:

$$P_{\boldsymbol{Y}_1,\boldsymbol{Y}_2|\boldsymbol{X}_1,\boldsymbol{X}_2} = P_{\boldsymbol{Y}_1|\boldsymbol{X}_1} P_{\boldsymbol{Y}_2|\boldsymbol{X}_1,\boldsymbol{X}_2}. \tag{1}$$

The open question for this channel is: given two independent messages $W_1 \in [1, 2^{n\mathsf{R}_1}]$ and $W_2 \in [1, 2^{n\mathsf{R}_2}]$, what are the rates R_1 and R_2 that can be reliably transmitted through this channel? Due to the importance of this problem it had attracted considerable attention throughout the years. Many results have been obtained; however, in general, the problem is still open. We refer the reader to recent overviews of the problem given in the introductory sections of [1] and [2].

The difficulty of this problem lies in the fact that we do not have a good understanding of the effect of a transmission on other (unintended) users. Moreover, as can be seen in the additive Gaussian white noise (AWGN) setting there is a rivalry between the two users [3], meaning that when one transmits at its maximum rate it also causes the maximum disturbance on the other user (a phenomenon known as the "worst additive noise" result [4]).

In this work we place an additional requirement on the interfering signal. Beyond its reliable decoding at its receiver we also require complete secrecy of this message at the interfered-with receiver. This additional requirement is relevant to many practical settings, in which our transmission can both be received by other, unintended receivers, but still we would like it to remain secure. As will be shown here this additional requirement provides interesting observations and many open questions.

We begin by formally stating the complete secrecy requirement:

$$\lim_{n\to\infty} \frac{1}{n} I\left(W_1; \boldsymbol{Y}_2\right) \to 0 \tag{2}$$

which assures complete secrecy of the interfering message at $\boldsymbol{Y}_2$. Note that due to this complete secrecy constraint we may consider only "weak interference". Figure 1 depicts the model.

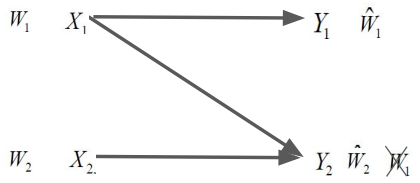

Fig. 1. The Z-Interference channel with a complete secrecy constraint for the interfering message at the interfered-with reciever.

This initial work focuses on the AWGN setting; however, as will be evident, many of the claims can be extended to discrete memoryless channels. Thus, we consider the following model for a single use of the channel:

$$\begin{aligned} Y_1 &= \sqrt{\mathsf{snr}_1} X_1 + N_1 \\ Y_2 &= \sqrt{\mathsf{snr}_2} X_2 + \sqrt{a\mathsf{snr}_1} X_1 + N_2 \end{aligned} \tag{3}$$

where N_1 and N_2 are standard additive Gaussian noise terms which can be assumed to be independent of each other and

The work of R. Bustin was supported in part by the women postdoctoral scholarship of Israel's Council for Higher Education (VATAT) 2014-2015, in part by the the U. S. Army Research Office under MURI Grant W911NF-11-1-0036, and in part by the U. S. National Science Foundation under Grants CMMI-1435778 and ECCS-1343210.

from channel use to channel use. They are also independent of the transmissions of the two users X_1 and X_2 which are independent of each other (no cooperation between the transmitters). We assume $a \in [0,1)$ which is the "weak interference" regime. There is also an average power constraint of 1 on both channel inputs.

In this work we distinguish between two scenarios. First, we do not limit either encoder, and allow stochastic encoders at both transmitters. Under this assumption we first examine the bounding box of the capacity region, that is, the maximum possible rates either user can obtain. This proves to be an interesting problem for which we can show, using the methods in [3] and [5] that the rate of the interfering message can increase beyond that obtained by simply having the interfered-with transmitter transmit Gaussian noise. Second, we consider a very probable case in which the interfered-with transmitter which has no secrecy requirements of its own is limited to a deterministic encoder. We observe that this limitation reduces the capacity region and provide a Sato-type [6] outer bound on its capacity region.

II. Stochastic Encoders - Capacity Region Bounding Box

The first question that comes to mind when considering the above problem concerns the bounding box of its capacity region. That is, we wish to know what is the maximum rate for either W_1 or W_2 regardless of the rate of the other user. For W_2 if we take $\mathsf{R}_1 = 0$ we comply with the secrecy constraint in the trivial sense (no information is transmitted), and in addition there is no interference; thus $\mathsf{R}_2 = \frac{1}{2}\mathsf{log}(1+\mathsf{snr}_2)$ can be achieved, which is, of course, the maximum possible rate. On the other hand, the maximum value of R_1 is an open problem. Examining (3) we can see that $\boldsymbol{Y}_2$ is a *degraded* version of $\boldsymbol{Y}_1$ (since $a \in [0,1)$), and thus we have that $\boldsymbol{X}_1 - \boldsymbol{Y}_1 - \boldsymbol{Y}_2$ is a Markov chain regardless of the distribution of $\boldsymbol{X}_2$. Using the wiretap result for a *degraded* channel [7] we have a single-letter expression

$$\mathsf{R}_{1,\max} = \max_{P_{X_1}P_{X_2}} \left\{ I\left(X_1;Y_1\right) - I\left(X_1;Y_2\right) \right\} \tag{4}$$

where the maximization is over both distributions, as Y_2 depends on X_2 as well.

Note that if P_{X_1} is a Gaussian distribution then the optimal choice for P_{X_2} is also Gaussian due to the "worst additive noise" lemma [4]. However, there is a dependence between the two distributions and they must be optimized jointly. In order to break this dependence one can invoke the entropy power inequality (EPI), which provides an upper bound that is attained with equality if and only if both X_1 and X_2 are Gaussian. However, attempting to optimize this upper bound results in a Gaussian distribution for X_1 but not for X_2. This observation leads us to the next result following the approach of Abbe and Zheng [5], a proof of which is given in the appendix.

Theorem 1. *For any* $\mathsf{snr}_1 > 0, \mathsf{snr}_2 > 0$ *and any* $a \in [0,1)$, $\mathsf{R}_{1,\max}$ *is obtained by non-Gaussian distributions in (4), meaning*

$$\mathsf{R}_{1,\max} > \frac{1}{2}\mathsf{log}(1+\mathsf{snr}_1) - \frac{1}{2}\mathsf{log}\left(1+\frac{a\mathsf{snr}_1}{1+\mathsf{snr}_2}\right). \tag{5}$$

III. Deterministic Interfered-With Encoder

In this section we restrict the encoder of the interfered-with transmitter to the class of deterministic encoders. Note that this transmitter has no secrecy constraints on its message, thus making this a very reasonable assumption. The advantage of this restriction is in allowing us to follow the approach of Sato [6] and Costa [8] and provide a good outer bound on the capacity of this channel. However, as we will show, this restriction, although reasonable from a practical viewpoint, reduces the capacity region of this channel.

We begin this section with the following result that extends the result of Costa [8] to our setting:

Lemma 1. *The Gaussian Z-Interference channel with secrecy constraint and a deterministic encoder for the message* W_2, *meaning* $H(\boldsymbol{X}_2|W_2) = 0$, *is equivalent, in the sense that they have the same capacity region, to the* degraded *Gaussian interference channel:*

$$\begin{aligned} \boldsymbol{Y}'_1 &= \sqrt{\mathsf{snr}_1}\boldsymbol{X}_1 + \sqrt{\frac{\mathsf{snr}_2}{a}}\boldsymbol{X}_2 + \boldsymbol{N}_1 \\ \boldsymbol{Y}'_2 &= \sqrt{\mathsf{snr}_1}\boldsymbol{X}_1 + \sqrt{\frac{\mathsf{snr}_2}{a}}\boldsymbol{X}_2 + \boldsymbol{N}_1 + \boldsymbol{N}'_2 \end{aligned} \tag{6}$$

where $\boldsymbol{N}_1$ *is as defined above, standard additive Gaussian noise, whereas* $\boldsymbol{N}'_2$ *is additive Gaussian noise of variance* $\frac{1-a}{a}$.

Proof: Following the proof of Costa [8] we refer to [8, Figure 6]. Note that the equivalence between [8, Figure 6-(a)] and [8, Figure 6-(c)] holds for the same reasons as in [8]. The equivalence to [8, Figure 6-(d)], the *degraded* Gaussian interference channel requires more delicacy. Note that as claimed in [8, Appendix A] the capacity region of [8, Figure 6-(a)] contains the capacity region of [8, Figure 6-(d)], with the additional secrecy constraints. This is due to the fact that $\boldsymbol{Y}_1$ is a better version than the equivalent output in the [8, Figure 6-(d)]. The reverse claim follows if we assume that $H(\boldsymbol{X}_2|W_2) = 0$ by following the proof in [8, Appendix A]. ∎

The above equivalence is limited to the case of deterministic encoders for the interfered-with transmitter. This transmitter is not the one transmitting a message that is required to be completely secure. Nonetheless, we will now show that this restriction limits the capacity region and is thus a sub-region of the capacity region of the original problem.

Theorem 2. *By restricting the encoder of the interfered-with user to a deterministic encoder we strictly reduce the capacity region.*

Proof: In order to show the above we show that the capacity region given the restriction to a deterministic encoder for the interfered-with transmitter does not contain a point

that can be achieved without this restriction. The point that we consider is the one obtained by $\mathsf{R}_2 = 0$, where $\boldsymbol{X}_2$ is simply Gaussian noise (random noise created ad-hoc in the transmitter, which is an "empty" stochastic encoder). Given that this is our choice of $\boldsymbol{X}_2$ it is evident that

$$\mathsf{R}_1 = \frac{1}{2}\mathsf{log}(1+\mathsf{snr}_1) - \frac{1}{2}\mathsf{log}\left(1+\frac{a\mathsf{snr}_1}{1+\mathsf{snr}_2}\right) \tag{7}$$

is achievable using a standard optimal code sequence for the Gaussian wiretap channel.

We now need to show that this is not attainable when we limit the encoder of the interfered-with transmission to a deterministic encoder. This observation also provides us with the exact bounding box of the capacity region of this limited case. Note that by limiting to a deterministic encoder and due to the fact that we have reliable communication of W_2 to $\boldsymbol{Y}_2$, we have the following equality in the limit, due to the requirement of complete secrecy:

$$\begin{aligned}
\mathsf{R}_{1,\max} &= \lim_{n\to\infty}\left[I\left(\boldsymbol{X}_1;\boldsymbol{Y}_1\right) - I\left(\boldsymbol{X}_1;\boldsymbol{Y}_2\right)\right] \\
&= \lim_{n\to\infty}\left[I\left(\boldsymbol{X}_1;\boldsymbol{Y}_1\right) - I\left(\boldsymbol{X}_1;\boldsymbol{Y}_2|\boldsymbol{X}_2\right)\right. \\
&\quad \left. + I\left(\boldsymbol{X}_2;\boldsymbol{Y}_2|\boldsymbol{X}_1\right) - I\left(\boldsymbol{X}_2;\boldsymbol{Y}_2\right)\right] \\
&= \lim_{n\to\infty}\left[I\left(\boldsymbol{X}_1;\boldsymbol{Y}_1\right) - I\left(\boldsymbol{X}_1;\boldsymbol{Y}_2|\boldsymbol{X}_2\right)\right] \\
&= \lim_{n\to\infty}\left[I\left(\boldsymbol{X}_1;\sqrt{\mathsf{snr}_1}\boldsymbol{X}_1+\boldsymbol{N}_1\right)\right. \\
&\quad \left. - I\left(\boldsymbol{X}_1;\sqrt{a\mathsf{snr}_1}\boldsymbol{X}_1+\boldsymbol{N}_2\right)\right]
\end{aligned} \tag{8}$$

where the second equality is due to reliable communication of W_2 and the deterministic encoder restriction $W_2 \to \boldsymbol{X}_2$. The last transition is due to the independence of $\boldsymbol{X}_1$ and $\boldsymbol{X}_2$ (no cooperation). Maximizing the above expression over $P_{\boldsymbol{X}_1}$ (it no longer depends on $P_{\boldsymbol{X}_2}$) gives us the maximum rate

$$\mathsf{R}_{1,\max} = \frac{1}{2}\mathsf{log}(1+\mathsf{snr}_1) - \frac{1}{2}\mathsf{log}(1+a\mathsf{snr}_1) \tag{9}$$

which is strictly less than (7). Thus, for this setting we know the bounding box is defined by the above and $\mathsf{R}_2 = \frac{1}{2}\mathsf{log}(1+\mathsf{snr}_2)$. Moreover, according to the results in [2] $\mathsf{R}_2 = \frac{1}{2}\mathsf{log}(1+\mathsf{snr}_2)$ is obtained when $\mathsf{R}_1 = 0$, since reliable decoding of $\boldsymbol{X}_1$ is required for the maximum R_2, and thus complete secrecy cannot be attained. In other words, the pair $(0, \frac{1}{2}\mathsf{log}(1+\mathsf{snr}_2))$ is a corner point of the capacity region in this setting. This concludes the proof. ∎

Given the above equivalence we have a *degraded* Gaussian interference channel. For this channel we wish to provide a Sato-type outer bound, meaning we wish to follow the approach in [6]. The approach in [6] was to observe that the *degraded* Gaussian interference channel is upper bounded by the Gaussian broadcast channel (BC) capacity since in the Gaussian BC the two transmitters cooperate and only have a general power constraint (may split the power between themselves as they wish). Thus, the specific power split of the *degraded* Gaussian interference channel is a special case of the Gaussian BC.

Our approach is to follow the same logic and employ the known results of the Gaussian BC with confidential messages (BCC), for which we have the capacity region [9]. This leads to the following result:

Theorem 3. *The capacity region of the Gaussian Z-interference channel with a secrecy constraint on the interfering message and a deterministic encoder at the interfered-with transmitter is contained in the following region:*

$$\begin{aligned}
(\mathsf{R}_1,\mathsf{R}_2) = \Bigg(&\frac{1}{2}\mathsf{log}\left(\frac{1+\beta(\mathsf{snr}_1+\mathsf{snr}_2/a)}{1+\beta a(\mathsf{snr}_1+\mathsf{snr}_2/a)}\right), \\
&\frac{1}{2}\mathsf{log}\left(\frac{1+a(\mathsf{snr}_1+\mathsf{snr}_2/a)}{1+\beta a(\mathsf{snr}_1+\mathsf{snr}_2/a)}\right)\Bigg) \\
\mathsf{R}_1 &\le \frac{1}{2}\mathsf{log}\left(1+\mathsf{snr}_1\right) - \frac{1}{2}\mathsf{log}(1+a\mathsf{snr}_1) \\
\mathsf{R}_2 &\le \frac{1}{2}\mathsf{log}\left(1+\mathsf{snr}_2\right)
\end{aligned} \tag{10}$$

for some $\beta \in [0,1]$.

As discussed in the proof of Theorem 2, the point $(0, \frac{1}{2}\mathsf{log}\left(1+\mathsf{snr}_2\right))$ is a corner point of the capacity region. However this is not a point on the above outer bound. Assume that

$$\mathsf{R}_2 = \frac{1}{2}\mathsf{log}\left(1+\mathsf{snr}_2\right) \tag{11}$$

then

$$\beta = \frac{a\mathsf{snr}_1}{(a\mathsf{snr}_1+\mathsf{snr}_2)(1+\mathsf{snr}_2)}. \tag{12}$$

Substituting the above in the bound on R_1 we obtain

$$\mathsf{R}_1 = \frac{1}{2}\mathsf{log}\left(1+\frac{\mathsf{snr}_1}{1+\mathsf{snr}_2}\right) - \frac{1}{2}\mathsf{log}\left(1+\frac{a\mathsf{snr}_1}{1+\mathsf{snr}_2}\right). \tag{13}$$

The other corner point of the above outer bound is when

$$\mathsf{R}_1 = \frac{1}{2}\mathsf{log}\left(1+\mathsf{snr}_1\right) - \frac{1}{2}\mathsf{log}(1+a\mathsf{snr}_1) \tag{14}$$

for which

$$\beta(a\mathsf{snr}_1+\mathsf{snr}_2) = a\mathsf{snr}_1. \tag{15}$$

Substituting the above in the bound on R_2 we obtain

$$\mathsf{R}_2 = \frac{1}{2}\mathsf{log}\left(1+\frac{\mathsf{snr}_2}{1+a\mathsf{snr}_1}\right). \tag{16}$$

This, of course, is an attainable point by using for W_1 a Gaussian wiretap code sequence, and for W_2 a Gaussian point-to-point code sequence. At $\boldsymbol{Y}_2$ we first consider $\boldsymbol{X}_1$ as additive Gaussian noise and decode $\boldsymbol{X}_2$ (W_2). After removing it, we still have for W_1 a Gaussian wiretap code sequence designed for complete secrecy at $\boldsymbol{Y}_2$.

In order to get a better feeling for the above outer bound, we compare it with three possible inner bounds. The first most basic inner bound is obtained by time-sharing between the two schemes that attain the corner points of the capacity region mentioned above. The second bound is the time/frequency division multiplexing (TDM/FDM) bound given in Lemma 2 and the third bound, given in Lemma 3, improves on the

TDM/FDM bound by allowing the interfered-with transmitter to transmit over both subbands.

Lemma 2. *The set of non-negative rate pairs* $(\mathsf{R}_1, \mathsf{R}_2)$ *satisfying*

$$\mathsf{R}_1 \leq \frac{\lambda}{2}\mathsf{log}\Big(1+\frac{\mathsf{snr}_1}{\lambda}\Big) - \frac{\lambda}{2}\mathsf{log}\Big(1+\frac{a\mathsf{snr}_1}{\lambda}\Big), \quad (17)$$

$$\mathsf{R}_2 \leq \frac{\bar{\lambda}}{2}\mathsf{log}\Big(1+\frac{\mathsf{snr}_2}{\bar{\lambda}}\Big), \quad (18)$$

in which $0 \leq \lambda \leq 1$ *and* $\bar{\lambda} = 1-\lambda$*, is achievable for the Gaussian Z-Interference channel with secrecy constraint and a deterministic encoder.*

Proof: This region is the TDM/FDM region. To achieve this region we divide the available time/frequency into two orthogonal parts, respectively proportional to λ and $\bar{\lambda}$. Then, let user 1 be the only active user for λ fraction of time/frequency. As a result, we will have a degraded Gaussian wiretap channel and the achievable rate of secure communication is given by (17). Note that the average SNR of transmitter 1 in the λ-subband is equal to $\frac{snr_1}{\lambda}$. Similarly, let user 2 transmit only for $\bar{\lambda}$ fraction of time/frequency. Then, (18) gives the achievable rate. ∎

We can improve the TDM/FDM inner bound of Lemma 2 by allowing the interfered-with transmitter to split its power over both subbands.

Lemma 3. *The set of non-negative rate pairs* $(\mathsf{R}_1, \mathsf{R}_2)$ *satisfying*

$$\mathsf{R}_1 \leq \frac{\lambda}{2}\mathsf{log}\Big(1+\frac{\mathsf{snr}_1}{\lambda}\Big) - \frac{\lambda}{2}\mathsf{log}\Big(1+\frac{a\mathsf{snr}_1}{\lambda}\Big), \quad (19)$$

$$\mathsf{R}_2 \leq \frac{\lambda}{2}\mathsf{log}\Big(1+\frac{\mathsf{snr}_{21}}{1+a\frac{\mathsf{snr}_1}{\lambda}}\Big) + \frac{\bar{\lambda}}{2}\mathsf{log}\Big(1+\mathsf{snr}_{22}\Big), \quad (20)$$

in which $0 \leq \lambda \leq 1$*,* $\bar{\lambda} = 1-\lambda$*, and* $\lambda\mathsf{snr}_{21} + \bar{\lambda}\mathsf{snr}_{22} = \mathsf{snr}_2$ *is achievable for the Gaussian Z-Interference channel with secrecy constraint and a deterministic encoder.*

Proof: Similar to the TDM/FDM inner bound, we divide the available time/frequency into two orthogonal parts proportional to λ and $\bar{\lambda}$. The main difference here is to split snr_2 into snr_{21} and snr_{22} such that $\lambda\mathsf{snr}_{21} + \bar{\lambda}\mathsf{snr}_{22} = \mathsf{snr}_2$ and let user 2 consume them in the λ and $\bar{\lambda}$ fraction of time/frequency, respectively. However, user 1 transmits only in the λ-subband. Therefore, in the λ-subband both users are active. Clearly, (19) is still achievable for user 1 since receiver 1 is free of interference. The achievable rate of user 2 has two terms, each corresponding to one of the subbands. In the λ-subband receiver 2 treats interference as noise to achieve $\mathsf{R}_{21} = \frac{1}{2}\mathsf{log}\big(1+\frac{\mathsf{snr}_{21}}{1+a\frac{\mathsf{snr}_1}{\lambda}}\big)$. In the $\bar{\lambda}$-subband user 2 is the only active user and thus the interference-free rate $\mathsf{R}_{22} = \frac{1}{2}\mathsf{log}\big(1+\mathsf{snr}_{22}\big)$ is achievable. Therefore, $\mathsf{R}_2 = \lambda\mathsf{R}_{21} + \bar{\lambda}\mathsf{R}_{22}$ is obtained for user 2 in (20). ∎

Figure 2 depicts both the Sato-type outer bound (dashed) and the three possible inner-bounds.

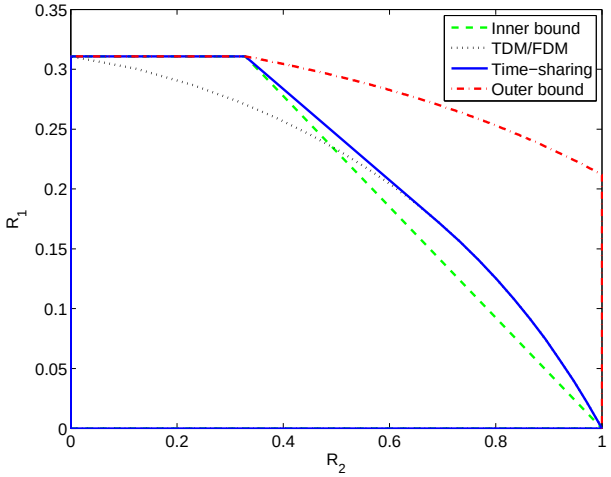

Fig. 2. The Sato-type outer bound (dash-dot line), the basic time-sharing inner bound (dashed), the TDM/FDM inner bound (dotted) and the improved TDM/FDM inner bound (solid).

APPENDIX

Sketch Proof of Theorem 1: We follow the approach proposed by Abbe and Zheng in [5] which examines the optimality of the Gaussian inputs by analysis of the information theoretic equation in the vicinity of the Gaussian input distributions using permutations depicted by Hermite polynomials.

The single-letter expression which we are considering is the following:

$$I(X_1;Y_1) - I(X_1;Y_2) = I\left(X_1;\sqrt{\mathsf{snr}_1}X_1+N_1\right) - I\left(X_1;\sqrt{a\mathsf{snr}_1}X_1+\sqrt{\mathsf{snr}_2}X_2+N_2\right).$$

Similar to [5] we denote the above function using

$$\begin{aligned} &S_{a,\mathsf{snr}_1,\mathsf{snr}_2,p}(X_1,X_2) \quad (21)\\ &= h(\sqrt{\mathsf{snr}_1}X_1+N_1) - h(N_1)\\ &\quad - h(\sqrt{a\mathsf{snr}_1}X_1+\sqrt{\mathsf{snr}_2}X_2+N_2) + h(\sqrt{\mathsf{snr}_2}X_2+N_2), \end{aligned}$$

where p is defined below. Now the idea is to examine the following function:

$$F_k(a,\mathsf{snr}_1,\mathsf{snr}_2,p) = \quad (22)$$
$$\lim_{\delta\to 0}\lim_{\epsilon\to 0}\frac{2}{\epsilon^2}\left[S_{a,\mathsf{snr}_1,\mathsf{snr}_2,p}(X_1,X_2) - S_{a,\mathsf{snr}_1,\mathsf{snr}_2,p}(X_1^G,X_2^G)\right]$$

where $X_1^G \sim g_p$, $X_2^G \sim g_p$, $X_1 \sim g_p(1+\epsilon\widetilde{H}_k)$ and $X_2 \sim g_p(1-\epsilon\widetilde{H}_k)$ with $\widetilde{H}_k$ defined in [5, Lemma 2] as a function of $H_k^{[p]}$ (and the $\delta H_{4k}^{[p]}$ correction term), the normalized Hermite polynomials for the Gaussian distribution having variance p, g_p. Recall from [5] that $\{H_k^{[p]}\}_{k\geq 0}$ is an orthonormal basis for $L_2(g_p;\Re)$. Moreover, $H_1^{[p]}$ and $H_2^{[p]}$ perturb a Gaussian distribution into another Gaussian distribution with a different first and second moments, respectively. For $k \geq 3$ the permutations move away from the Gaussian distribution. To

simplify notation we denote the Hermite polynomials as H_k whenever the variance p is clear from context.

Given the above we wish to analyze the behavior of the function $F_k(a, \mathsf{snr}_1, \mathsf{snr}_2, p)$ for $k \geq 3$. We have three differential entropies to consider. We begin with $h(\sqrt{a\mathsf{snr}_1}X_1 + \sqrt{\mathsf{snr}_2}X_2 + N_2)$. As shown in [5, Equation (20)] the density of $\sqrt{a\mathsf{snr}_1}X_1 + \sqrt{\mathsf{snr}_2}X_2 + N_2$ is given by

$$g_{a\mathsf{snr}_1 p}(1 + \epsilon\left[H_k + \delta H_{4k}\right]) \star g_{\mathsf{snr}_2 p}(1 - \epsilon\left[H_k - \delta H_{4k}\right]) \star g_1 \tag{23}$$

where $\star$ denotes the convolution operator. From [5, Theorem 1] the above is equal to

$$\begin{aligned} &g_{a\mathsf{snr}_1 p + \mathsf{snr}_2 p + 1}\left(1 + \epsilon\left\{\left[\left(\frac{a\mathsf{snr}_1 p}{a\mathsf{snr}_1 p + \mathsf{snr}_2 p + 1}\right)^{\frac{k}{2}} H_k + \right.\right.\right. \\ &\delta\left(\frac{a\mathsf{snr}_1 p}{a\mathsf{snr}_1 p + \mathsf{snr}_2 p + 1}\right)^{2k} H_{4k}\Bigg] \\ &-\Bigg[\left(\frac{\mathsf{snr}_2 p}{a\mathsf{snr}_1 p + \mathsf{snr}_2 p + 1}\right)^{\frac{k}{2}} H_k \\ &\left.\left.\left.-\delta\left(\frac{\mathsf{snr}_2 p}{a\mathsf{snr}_1 p + \mathsf{snr}_2 p + 1}\right)^{2k} H_{4k}\right] - \epsilon L\right\}\right) \end{aligned} \tag{24}$$

where

$$L = \frac{g_{a\mathsf{snr}_1 p}\left[H_k + \delta H_{4k}\right] \star g_{\mathsf{snr}_2 p}\left[H_k - \delta H_{4k}\right] \star g_1}{g_{a\mathsf{snr}_1 p + \mathsf{snr}_2 p + 1}}. \tag{25}$$

Using [5, Lemma 3] one can show that L is a linear combination of several Hermite polynomials H_ℓ of power $a\mathsf{snr}_1 p + \mathsf{snr}_2 p + 1$ with $\ell \geq 2k$. Thus, the density of $\sqrt{a\mathsf{snr}_1}X_1 + \sqrt{\mathsf{snr}_2}X_2 + N_2$ can be written as a Gaussian $g_{a\mathsf{snr}_1 p + \mathsf{snr}_2 p + 1}$ perturbed by the direction H_k on the order of ϵ and several H_ℓ's with $\ell \geq 2k$ on the order of ϵ^2. Using [5, Lemma 2] and denoting $Y_2 = \sqrt{a\mathsf{snr}_1}X_1 + \sqrt{\mathsf{snr}_2}X_2 + N_2$ and $Y_2^G = \sqrt{a\mathsf{snr}_1}X_1^G + \sqrt{\mathsf{snr}_2}X_2^G + N_2$, we have

$$\begin{aligned} &h(\sqrt{a\mathsf{snr}_1}X_1 + \sqrt{\mathsf{snr}_2}X_2 + N_2) = \\ &h(\sqrt{a\mathsf{snr}_1}X_1^G + \sqrt{\mathsf{snr}_2}X_2^G + N_2) - D(Y_2||Y_2^G) \end{aligned} \tag{26}$$

and using [5, Lemma 1] we have

$$\begin{aligned} D(Y_2||Y_2^G) &= \frac{\epsilon^2}{2}o(\delta) \\ &+ \frac{\epsilon^2}{2}\left((a\mathsf{snr}_1)^{\frac{k}{2}} - (\mathsf{snr}_2)^{\frac{k}{2}}\right)^2 \left(\frac{p}{a\mathsf{snr}_1 p + \mathsf{snr}_2 p + 1}\right)^k \end{aligned} \tag{27}$$

Following similar steps we have that $h(\sqrt{\mathsf{snr}_1}X_1 + N_1)$ is

$$h(\sqrt{\mathsf{snr}_1}X_1^G + N_1) - \frac{\epsilon^2}{2}\left(\frac{\mathsf{snr}_1 p}{\mathsf{snr}_1 p + 1}\right)^k + \frac{\epsilon^2}{2}o(\delta) \tag{28}$$

and $h(\sqrt{\mathsf{snr}_2}X_2 + N_2)$ is

$$h(\sqrt{\mathsf{snr}_2}X_2^G + N_2) - \frac{\epsilon^2}{2}\left(\frac{\mathsf{snr}_2 p}{\mathsf{snr}_2 p + 1}\right)^k + \frac{\epsilon^2}{2}o(\delta). \tag{29}$$

Putting everything together we have that

$$S_{a,p}(X_1, X_2) - S_{a,p}(X_1^G, X_2^G) \tag{30}$$

$$\begin{aligned} &= \frac{\epsilon^2}{2}\left[\left(\frac{\mathsf{snr}_1 p}{\mathsf{snr}_1 p + 1}\right)^k + \left(\frac{\mathsf{snr}_2 p}{\mathsf{snr}_2 p + 1}\right)^k \right. \\ &\left. - \left((a\mathsf{snr}_1)^{\frac{k}{2}} - (\mathsf{snr}_2)^{\frac{k}{2}}\right)^2 \left(\frac{p}{a\mathsf{snr}_1 p + \mathsf{snr}_2 p + 1}\right)^k\right] + \frac{\epsilon^2}{2}o(\delta). \end{aligned}$$

As noted above, the condition for a non-Gaussian distribution to improve on the Gaussian one is that there exists some $k \geq 3$ for which

$$\begin{aligned} &\left(\frac{\mathsf{snr}_1 p}{\mathsf{snr}_1 p + 1}\right)^k + \left(\frac{\mathsf{snr}_2 p}{\mathsf{snr}_2 p + 1}\right)^k \\ &- \left((a\mathsf{snr}_1)^{\frac{k}{2}} - (\mathsf{snr}_2)^{\frac{k}{2}}\right)^2 \left(\frac{p}{a\mathsf{snr}_1 p + \mathsf{snr}_2 p + 1}\right)^k > 0. \end{aligned}$$

Moreover, since we have snr_1 and snr_2 we can take $p = 1$ in the above. Examining this expression (with $p = 1$) we observe that we can lower bound it with

$$\left(\frac{\mathsf{snr}_1}{\mathsf{snr}_1 + 1}\right)^k + \left(\frac{\mathsf{snr}_2}{\mathsf{snr}_2 + 1}\right)^k - \frac{a^k\mathsf{snr}_1^k + \mathsf{snr}_2^k}{(a\mathsf{snr}_1 + \mathsf{snr}_2 + 1)^k}.$$

Noticing that

$$\left(\frac{\mathsf{snr}_2}{\mathsf{snr}_2 + 1}\right)^k - \frac{\mathsf{snr}_2^k}{(a\mathsf{snr}_1 + \mathsf{snr}_2 + 1)^k} \geq 0 \tag{31}$$

and for any $a \in [0, 1]$ also

$$\left(\frac{\mathsf{snr}_1}{\mathsf{snr}_1 + 1}\right)^k - \frac{a^k\mathsf{snr}_1^k}{(a\mathsf{snr}_1 + \mathsf{snr}_2 + 1)^k} \geq 0 \tag{32}$$

as it is a monotonically decreasing function in $a \in [0, 1]$ and for $a = 1$ it is non-negative. Thus, we can conclude that for any set of parameters $\mathsf{snr}_1 > 0, \mathsf{snr}_2 > 0$ and $a \in [0, 1)$ a non-Gaussian distribution would outperform the Gaussian one in the maximization problem given in (4). This concludes the proof. ■

REFERENCES

[1] I. Sason, "On the corner points of the capacity region of a two-user Gaussian interference channel," *IEEE Transactions on Information Theory*, vol. 61, no. 7, pp. 3682–3697, July 2015.

[2] R. Bustin, H. V. Poor, and S. Shamai (Shitz), "The effect of maximal rate codes on the interfering message rate," submitted to the *IEEE Transactions on Information Theory, April 2015*, 2015, arXiv:1404.6690.

[3] E. A. Abbe and L. Zheng, "A coordinate system for Gaussian networks," *IEEE Transactions on Information Theory*, vol. 58, no. 2, pp. 721–733, February 2012.

[4] S. N. Diggavi and T. M. Cover, "The worst additive noise under a covariance constraint," *IEEE Transactions on Information Theory*, vol. 47, no. 7, pp. 3072–3081, November 2001.

[5] E. A. Abbe and L. Zheng, "Coding along Hermite polynomials for interference channels," in *Proc. IEEE Information Theory Workshop, (ITW 2009)*, pp. 584–588, Taormina, Sicillia, Italy, 11-16 October 2009.

[6] H. Sato, "On degraded Gaussian two-user channels," *IEEE Transactions on Information Theory*, vol. 24, no. 5, pp. 637–640, September 1977.

[7] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, October 1975.

[8] M. H. M. Costa, "On the Gaussian interference channel," *IEEE Transactions on Information Theory*, vol. 31, no. 5, pp. 607–615, September 1985.

[9] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Secure communication over fading channels," *IEEE Transactions on Information Theory, Special Issue on Information Theoretic Security*, vol. 54, no. 6, pp. 2470–2492, June 2008.